UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
KWG PARTNERS, LLC,

Plaintiff,

-against-

ORDER

JEREMY SIGEL, JNS REALITY, JOHN DOES 1-13,

11-CV-2890 (NGG) (JMA)

Defendants.
----------X

A P P E A R A N C E S:

Evan M. Newman
Joseph Zelmanovitz
Stahl & Zelmanovitz
747 Third Avenue, Suite 33b
New York, NY 10017
Attorney for Plaintiff

AZRACK, **United States Magistrate Judge:**

On June 16, 2011, KWG Partners, LCC ("plaintiff") filed suit against Jeremy Sigel, JNS Reality, and John Does 1–13 alleging violations of the Computer Fraud and Abuse Act, the Stored Communications Act, trespass to chattels, theft of trade secrets, fraud, misappropriation, breach of contract, conversion, and unfair competition. See Compl. ¶¶ 47–121, ECF No. 1. Plaintiff now moves for expedited, pre-answer discovery in the form of third-party subpoenas to be issued to internet service providers ("ISPs") in order to obtain subscriber information affiliated with certain internet protocol ("IP") addresses. For the reasons set forth below, the motion is denied without prejudice and with leave to renew after the action has been joined.

I. BACKGROUND

Plaintiff offers a service through a website that "provides paid users with up to the minute updates of any violations, repair orders[,] and complaints lodged against their buildings by

multiple city agencies . . . ." Compl. ¶ 12. The service is "designed to warn building management before [a] complaint snowballs into multiple violations, allowing management time to fix the problem before City inspectors appear." Compl. ¶ 17. After paying a fee, customers are assigned usernames and passwords to access the site. Compl. ¶¶ 12, 23. The terms of use, which every user is required to accept, prevent the customer from using the service for anything other his own internal business purpose. Compl. ¶¶ 25, 27. Defendant Sigel purchased one year of the service, and was assigned a username and password. Compl. ¶ 33–34.

According to plaintiff, it began noticing that Sigel's account was being accessed in a manner inconsistent with a single user. Compl. ¶ 37. In particular, the system was accessed via Sigel's username and password by thirteen unique IP addresses, and these IP addresses were located in "diverse geographic locations." Compl. ¶¶ 37–38. From this evidence, plaintiff surmises that Sigel "unlawfully shared his username and password with other users, in direct breach of the Terms of Use . . . ." Compl. ¶ 39. Further, based on the rough geographic location of some of the IP addresses, plaintiff believes that Sigel shared his username and password with a competitor of plaintiff. Compl. ¶ 44. On April 4, 2011, plaintiffs froze Sigel's account. Compl. ¶ 46. Plaintiff now moves for expedited discovery in hopes of ascertaining subscriber information affiliated with the IP addresses from non-party ISPs.

II. DISCUSSION

Courts in the Second Circuit employ two tests for determining the propriety of an expedited discovery request. The first is a "reasonableness standard." See Keybank, Nat'l Assoc. v. Quality Pay-Roll Sys., Inc., No. 06-CV-3013, 2006 WL 1720461, at *4 (E.D.N.Y. June 22, 2006) (citation omitted). The second is a four-factor test laid out in Notaro v. Koch, 95

F.R.D. 403 (S.D.N.Y. 1982). For the reasons set out below, I find that plaintiff's motion fails under either standard.

The reasonableness standard "requires the party seeking the discovery to prove that the requests are reasonable under the circumstances." Keybank, 2006 WL 1720461, at *4. Here, plaintiff alleges that its proprietary data was unlawfully accessed by a user or group of users, all of whom employed the same username and password. This does not appear to be a case of ongoing "hacking," but rather the alleged overuse of a single username and password. Any harm resulting from this allegedly improper access should have been halted when the account was frozen. Further, to the extent plaintiff argues that the harm is ongoing because the perpetrators could be continuing to use any ill-gained data, the perpetrators would already have been in possession of this data for almost three months at the time the motion was filed. The horse, as it were, is already out of the barn. The additional harm, if any, that could be caused in the short period between now and when the action is joined is outweighed by the general judicial disinclination to rule on ex parte requests. See Schiller v. City of New York, No. 04-CV-7922, 2008 WL 1777848, at *5 (S.D.N.Y. Apr. 14, 2008). Thus, because the improper access has been halted, and the mere possibility of some additional harm does not merit pre-answer, ex parte discovery, plaintiff fails to demonstrate that the request is reasonable under the circumstances.

Under the four-factor Notaro test, a plaintiff must demonstrate:

> (1) irreparable injury; (2) some probability of success on the merits; (3) some connection between the expedited discovery and the avoidance of irreparable injury, and (4) some evidence that the injury that will result without expedited discovery looms greater than the injury the defendant will suffer if the expedited relief is granted.

Notaro, 95 F.R.D. at 405. The Second Circuit defines irreparable harm as "certain and imminent harm for which a monetary award does not adequately compensate." Wisdom Import Sales Co.,

L.L.C. v. Labatt Brewing Co., Ltd., 339 F.3d 101, 113–14 (2d Cir. 2003). Here, plaintiff fails to demonstrate that it will suffer irreparable injury if discovery is not expedited. Plaintiff claims that it risks irreparable harm because "without knowing the identity of the hackers, [it] cannot adequately protect its system or ensure that its proprietary data is not used in the market . . . ." Pl.'s Letter Mot. for Disc. 3, ECF No. 2. First, because the allegedly improper access was limited to the sharing of a single username and password, the freeze of that account should "adequately protect" the system. Second, plaintiff offers no explanation why—assuming the alleged perpetrators are improperly in possession of data—the ensuing injury could not be adequately recompensed with monetary damages. Therefore, because plaintiff fails to demonstrate irreparable harm, I need not discuss the three remaining elements, and plaintiff's motion is denied without prejudice.

Nothing above, however, is meant to imply that I believe the subscriber information is not discoverable. Plaintiff gives no reason to believe that the ISPs will not have the information being sought after the defendants have a chance to respond to the complaint. Therefore, plaintiff is granted leave to renew this request for third-party subpoenas once the matter has been joined.

III. CONCLUSION

For the foregoing reasons, plaintiff's request for expedited discovery is denied without prejudice and with leave to renew after the matter has been joined.

SO ORDERED.

Dated: July 14, 2011
Brooklyn, New York

/s/
JOAN M. AZRACK
UNITED STATES MAGISTRATE JUDGE